4

Guidance™ SOFTWARE

October 7, 2003

Public Information Room
Office of the Comptroller of the Currency
250 E Street, SW, Mailstop 1-5
Washington, DC 20219
ATTN: Docket No. 03-18

Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551
ATTN: Docket No. OP-115

Steven F. Hanft
Legal Division, Room MB-3064
Federal Deposit of Insurance Corporation
550 17th Street, NW
Washington, DC 20429

Information Collection Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
ATTN: Docket No. 03-35

Re: Joint Notice of Proposed Guidelines

Dear Sirs or Madams:

These comments are submitted on behalf of Guidance Software, Inc. in response to the Joint Notice of proposed guidance, entitled Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice ("the proposed guidance"), issued by the Office of the Comptroller of the Currency ("OCC"), the Federal Deposit of Insurance Corporation ("FDIC"), the Board of Governors of the Federal Reserve System ("Federal Reserve"), and the Office of Thrift Supervision ("OTS") (collectively, the "Agencies"). The proposed guidance interprets section 501 (b) of the Gramm-Leach-Bliley Act and the Interagency Guidelines Establishing Standards for Safeguarding Customer Information and describes the Agencies' expectations regarding the response programs that a financial institution should develop and apply to address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer.

Guidance Software strongly supports the proposed guidance. Internal and external threats to the security of customer information often lead to the misuse of such information. Financial institutions must be required to develop a response program to protect against risks associated with these threats. The proposed guidelines include important measures to protect customer information systems maintained by financial institutions and its service providers. A response program ensures that each financial institution can quickly respond to incidents involving the unauthorized access or use of customer information. The proposed guidelines properly set forth the methods used to access, collect, store, use, transmit, and protect customer information. They include crucial requirements that regulatory and law enforcement agencies are notified when financial institutions become aware of an incident involving unauthorized access to or use of customer information. Furthermore, the proposed guidance clearly establish the corrective measures that must be taken to protect customers whose accounts were accessed without authorization, including notifying affected customers in a timely manner.

The proposed guidance, however, should also require financial institutions to establish effective means for collecting, preserving, and authenticating computer evidence in a form admissible in court. A regulated institution, as part of its response process, should have an effective computer forensics capability in order to investigate and mitigate computer security incidents. The leading international financial standards-setting institution, the Basel Committee on Banking Supervision[1] (the "Basel Committee"), has, like the Agencies' proposed guidance, realized that "[e]ffective incident response mechanisms are . . . critical to minimise operational, legal and reputational risks arising from internal and external attacks."[2] The Basel Committee has acknowledged the importance of computer forensics in its risk management standards for electronic banking, and in collecting evidence required for legal action. In its paper entitled "Risk Management for Electronic Banking", the Basel Committee set forth fourteen risk management principles, which urge banks to establish effective incident response capabilities. Principle 14 recommends that in implementing effective response to unforeseen incidents, banks should develop a "process for collecting and preserving forensic evidence to facilitate appropriate post-mortem reviews of any e-banking incidents, as well as to assist in the prosecution of attackers."[3]

The International Organization for Standardization ("ISO") also supports the use of computer forensics in responding to computer security incidents. In December 2000, ISO formally adopted a "code of practice for information security" ("ISO 17799"). ISO 17799 has emerged as one of the most widely recognized information security standards in the world.[4] Under ISO 17799, a financial institution that at has suffered a security incident must properly collect evidence for a variety or purposes, including internal problem analysis and for use as evidence in relation to a potential breach of contract, breach of regulatory requirements or in the event of civil or criminal proceedings.[5] ISO 17799 explicitly notes that a financial institution "should ensure that their information systems comply" with the requirements applicable to the production of admissible evidence.[6] Indeed, "[t]o achieve quality and completeness of the evidence, a strong evidence trail is needed."[7] Thus, ISO 17799 calls on financial institutions to use computer forensics to preserve the admissibility of evidence: "For information on computer media: copies of any removable media, information on hard disks or in memory should be taken to ensure availability. The log of all actions during the copying process should be kept . . ."[8] If a financial institution does not have the tools necessary to collect evidence in manner that preserves its admissibility, it risks compromising its legal (and hence its financial) position:

> When an incident is first detected, it may not be obvious that it will result in possible court action. Therefore, the danger exists

> that necessary evidence is destroyed accidentally before the seriousness of the incident is realized.[9]

A financial institution can minimize this danger by employing the best computer forensics tools available in its response to a security incident.

As discussed above, a broad computer forensics capability, as well as proper procedures and practices, is crucial for the referral and reporting of computer security incidents to law enforcement and federal regulatory agencies. When critical computer evidence is not properly preserved and handled by a regulated institution, it becomes difficult for law enforcement to successfully prosecute the matter, or for regulatory authorities to analyze the situation effectively. Computer forensics assists in preserving records and other evidence, and prevent the tampering of evidence that may be required in a criminal or civil legal action.

In sum, Guidance Software, Inc. supports the proposed interagency guidelines, but strongly recommends that the guidelines incorporate the need for institutions to collect properly preserved evidence. Computer forensics has proven useful in preserving records and preventing the tampering of evidence to ensure its admissibility in court. The Basel Committee and ISO 17799 have recommended the use of computer forensics in collecting evidence to support a legal action, whether civil or criminal.

Guidance Software, Inc. appreciates this opportunity to submit comments on the Joint Notice and hopes that its comments will be taken into consideration by the Agencies developing the final guidelines. If you have any questions regarding the matters discussed in this letter, please do not hesitate to contact us.

Sincerely,

Guidance Software, Inc. By:

Victor Limongelli, General Counsel
Sharon Tom, J.D.

---

[1] The Basel Committee on Banking Supervision was established in 1974 by the governors of the G10 central banks (Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom and the United States). Members also included non-central bank supervisory authorities and are mainly, but not exclusively, from G10 countries. It provides a forum for regular cooperation on banking supervisory matters. Over recent years, it has developed increasingly to a standard-setting body on all aspects of banking supervision.
[2] "Risk Management for Electronic Banking," at 3, available at: http://www.bis.org/publ/bcbs98.pdf
[3] Id. at 21.
[4] Symantec Advantage, Winter 2002, Issue 13.
[5] ISO 17799, § 6.3.1.
[6] Id., § 12.1.7.2.
[7] Id., § 12.1.7.3.
[8] Id.
[9] Id.